Maturity Framework for Assuring Resiliency Under Stress

Don O’Neill [vita[1]]

2008-07-11

Managing assurance is to reason about the emergent properties of large complex software-intensive systems; to take action to steer enterprise commitment towards their assurance; and to guide buyers, users, and the public in setting their level of confidence in these systems and systems of systems. The purpose of this article is to specify a framework for assuring the resiliency of the critical infrastructure through a management, process, and engineering framework of capabilities and solutions along with the model-based business, technical, and operational claims, arguments, and evidence useful in its assessment.

The nation’s critical infrastructure is vulnerable to natural disasters and cyber security attacks [CSTB 2007[11], DHS 2003[12], EMP 2004[13], Hoglund 2004[14], Larstan 2005[15], Miller 2008[16]]. Rather than simply focusing on protection and assurance measures as a response to known vulnerabilities and threats, it is necessary to elevate the focus to resiliency.

Resiliency is the ability to anticipate, avoid, withstand, minimize, and recover from the effects of adversity, whether natural or man-made, under all circumstances of use. Resiliency applied to the nation’s critical infrastructure is trustworthiness under stress and spans high availability, continuous operations, and disaster recovery. The operations within the industry sectors of the critical infrastructure are diverse and complex. These operations are evolving into large systems of systems. In normal times these operations may operate satisfactorily in a loosely coupled arrangement. However, for these operations to be resilient under stress, more than a loosely coupled arrangement is required.

A concerted action program is needed to break out of the current state. Measuring maturity in the assurance of resiliency under stress throughout the critical infrastructure would help public and private partners assess and manage cyber security risk and would accelerate the paradigm shift from critical infrastructure

[1] http://buildsecurityin.us-cert.gov/bsi/about_us/authors/681-BSI.html (O'Neill, Don)
[2] #dsy1016-BSI_basedef
[3] #dsy1016-BSI_framework
[4] #dsy1016-BSI_lvl2
[5] #dsy1016-BSI_lvl3
[6] #dsy1016-BSI_lvl4
[7] #dsy1016-BSI_lvl5
[8] #dsy1016-BSI_sumry
[9] #dsy1016-BSI_appx
[10] #dsy1016-BSI_tools
[11] #dsy1016-BSI_CSTB07
[12] #dsy1016-BSI_DHS03
[13] #dsy1016-BSI_EMP04
[14] #dsy1016-BSI_Hoglund04
[15] #dsy1016-BSI_Larstan05
[16] #dsy1016-BSI_Miller08

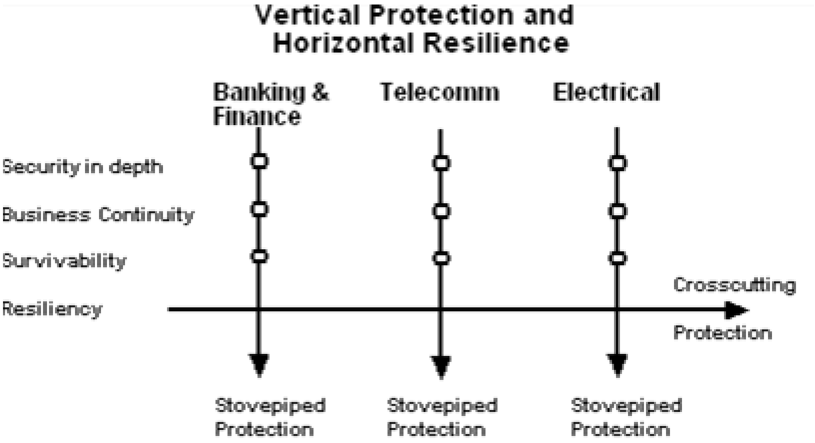
protection to critical infrastructure resilience. A resiliency maturity framework would drive the business case and enterprise commitment towards the assurance of software security in depth, business continuity, system survivability, and system of systems resiliency.

The result would improve both security and competitiveness. The enterprise that achieved resilience would boost its reputation and enhance the value of its brand. Being resilient would pay direct dividends to competitiveness. Achieving maturity in the assurance of resiliency throughout the critical infrastructure would help safeguard the nation's critical infrastructure and advance its global competitiveness.

Base Definition of Resiliency

The attribute of resiliency is an emerging property of large complex software-intensive systems. As the president of the Center for National Software Studies, I composed a base definition of *resiliency* that is not limited as to scale, does not preclude the possibility for avoiding the condition or situation that brings impact or shock, does not limit the focus to a means like risk management, and does not limit the focus to enumerated outcomes like cost effective or timely restoration. Accordingly, the base definition of resilience that I advocate is, as stated above, *the ability to anticipate, avoid, withstand, minimize, and recover from the effects of adversity, whether natural or man-made, under all circumstances of use.* In applying the base definition to a particular situation, it is permissible and required to constructively instantiate it for targeted scale, impact expected, means employed, and outcome anticipated.

Figure 1. Vertical protection and horizontal resilience



A defined engineering challenge of adopting resilience throughout the nation's critical infrastructure is needed. The recovery time objectives among industry sectors must be coordinated [O'Neill 2006b[17]], interoperability of information sharing and platform operations must be assured, distributed supervisory control protocols must be in place, and operation sensing and monitoring must be embedded. These crosscutting capabilities cannot be expected to evolve in a loosely coupled environment. They must be holistically specified, architected, designed, implemented, and tested if they are to operate with resilience under stress. A management, process, and engineering maturity framework is necessary to advance the assurance of software security, business continuity, system survivability, and system of system resiliency capabilities (Figure 1).

Crosscutting effects stem from dependent relationships. Some dependent relationships are planned and intended interactions between industry sectors, such as financial transactions embedded in telecommunications, electrical, transportation, and medical operations. Other dependent relationships are indirect and stem from outsourced commoditized services that bring with them opportunities for common single point failures among industry sectors, such as the Internet, the Global Positioning System, Federal Express, IBM, and Microsoft [Miller 2008[18]].

[17] #dsy1016-BSI_ONeill06b
[18] #dsy1016-BSI_Miller08

Maturity Framework for Assuring Resiliency Under Stress

The Maturity Framework for Assuring Resiliency Under Stress is intended to drive the business case and enterprise commitment towards the assurance of software security, business continuity, system survivability, and system of systems resiliency [CMMI 2006[20]].

The framework serves as a road map to assist reasoning about the software security decision process, to guide the selection of models appropriate for the enterprise, and to assist in their instantiation using local factors that best characterize the business environment and enterprise culture so as to achieve the best possible outcome. The framework will nudge the adopting organization towards the progressive assurance of software security, business continuity, system survivability, and system of systems resiliency capabilities.

Business case models provide a basis for rational action to assist understanding, constructing, implementing, verifying, and overseeing the enterprise assurance of software trustworthiness and security [O’Neill 2007b[21]]. Building security in has two important dimensions, business and technical. On the one hand, the Business Considerations Overview (Figure 2) illustrates the need to reconcile global software competitiveness and resiliency under stress. On the other hand, the Layers of Concern diagram (Figure 3) illustrates the technical depth involved. Business case models provide the means to unify and mutually reinforce these dimensions in building security into the software product foundation, the technology infrastructure, and the strategic management operation of the enterprise [O’Neill 2007a[22]].

Several contrasting perspectives must be considered in developing the business case:

1. It matters whether security is viewed as a cost or an investment.
2. It matters whether security solutions are viewed as commoditized or strategic.
3. It matters whether an organization seeks only protection or strives to achieve resilience.
4. It matters whether the security approach is inward looking and limited to a single system or outward looking to the system of systems of the critical infrastructure and its dependencies.

Figure 2. Business considerations overview

[20] #dsy1016-BSI_CMMI06
[21] #dsy1016-BSI_ONeill07b
[22] #dsy1016-BSI_ONeill07a

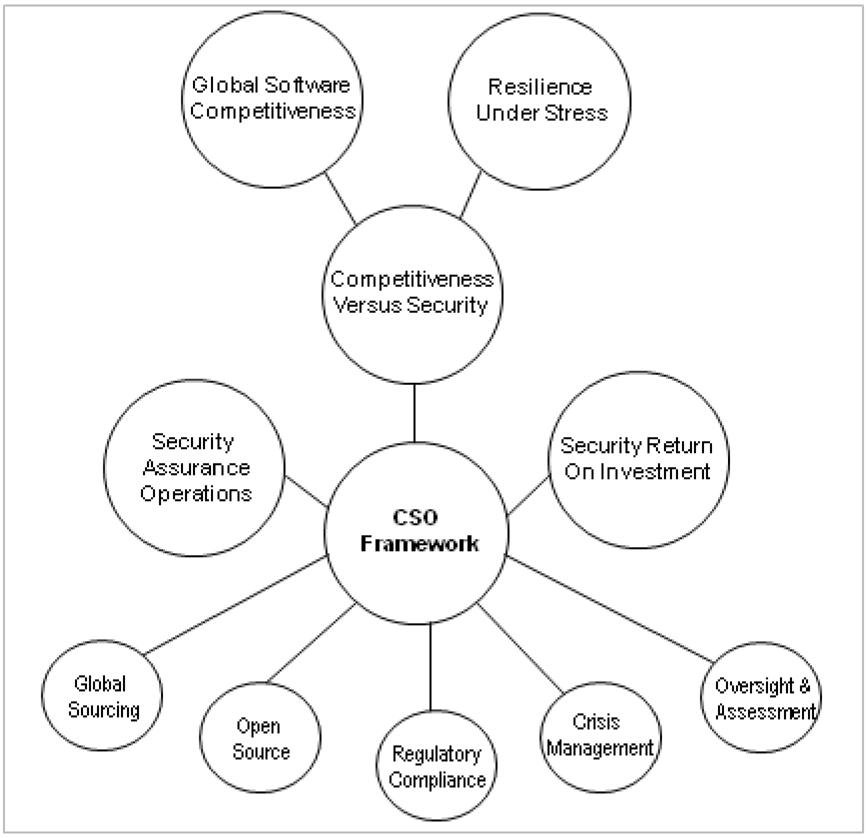
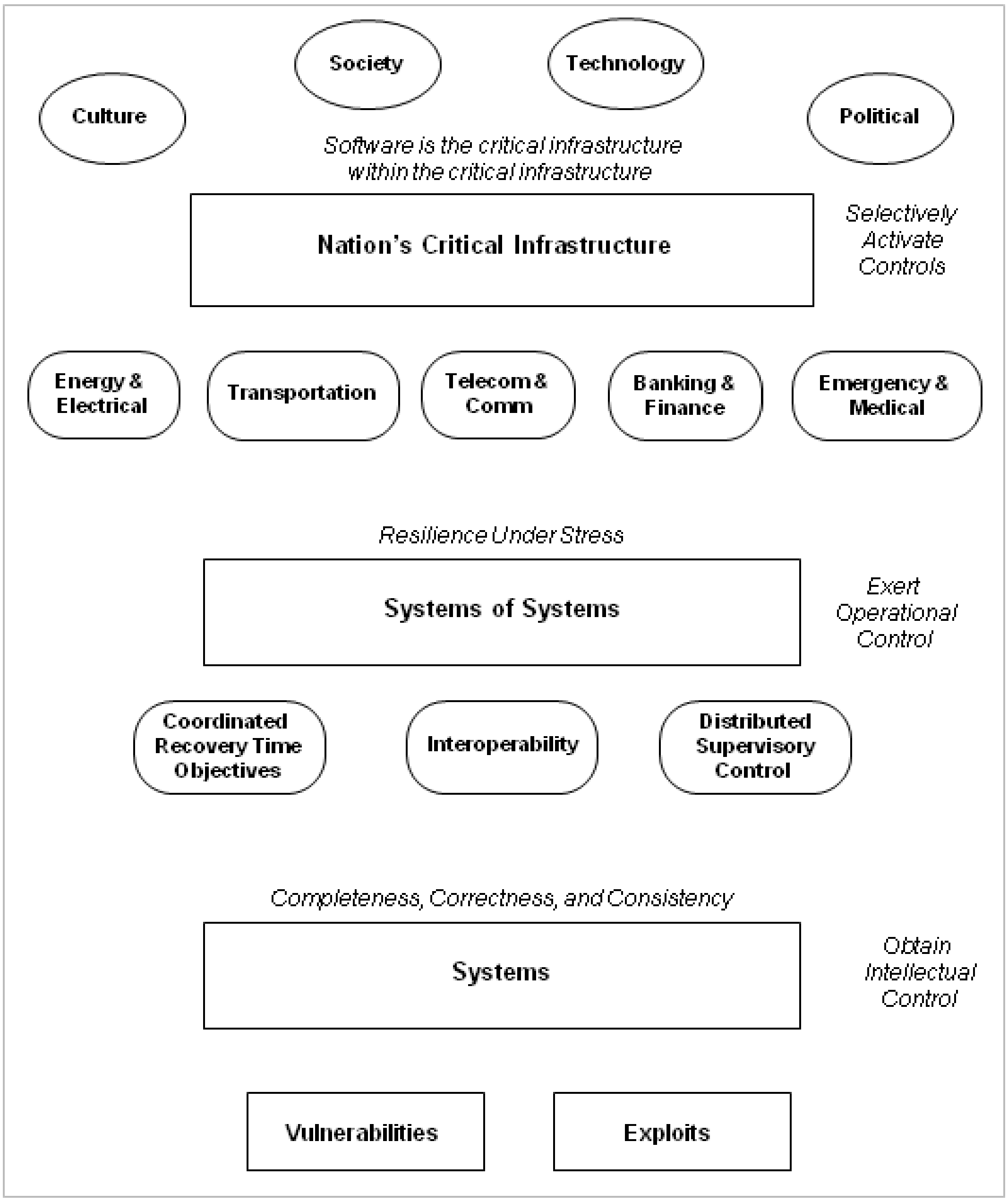


Figure 3. Layers of concern


Culture
Society
Technology
Political
Software is the critical infrastructure within the critical infrastructure
Nation's Critical Infrastructure
Selectively Activate Controls
Energy & Electrical
Transportation
Telecom & Comm
Banking & Finance
Emergency & Medical
Resilience Under Stress
Systems of Systems
Exert Operational Control
Coordinated Recovery Time Objectives
Interoperability
Distributed Supervisory Control
Completeness, Correctness, and Consistency
Systems
Obtain Intellectual Control
Vulnerabilities
Exploits

To achieve maturity in the assurance of resiliency under stress, the enterprise must satisfy the goal-based argument at each of five levels by enacting the focus areas at those levels. The levels and focus areas are as follows and also as depicted in Figure 4 (Level 1 is shown as a likely starting point):

Level 1 Ad Hoc

- State of Affairs: Inability to advance and exhibiting evidence of apathy, denial, management inaction, and lack of engineering know-how.
- Issue Areas: Apathy, State of Denial, Management Inaction, Lack of Engineering Know-How.

Level 2 Enterprise Security Commitment Management

- Goal: Demonstrate commitment to security assurance through strategic management, internal processes, and defense in depth.
- Focus Areas:Global Software Competitiveness, Competitiveness Versus Security, CSO Leadership Program, Security Return on Investment, Security Assurance Operations

Level 3 Enterprise Business Continuity Process Maturity

- Goal: Demonstrate business continuity assurance through compliance management, external processes, and product engineering.
- Focus Areas: Global Sourcing, Open Source, Regulatory Compliance, Crisis Management, Aspect Oversight & Assessment, Security Assurance Evaluation Tools

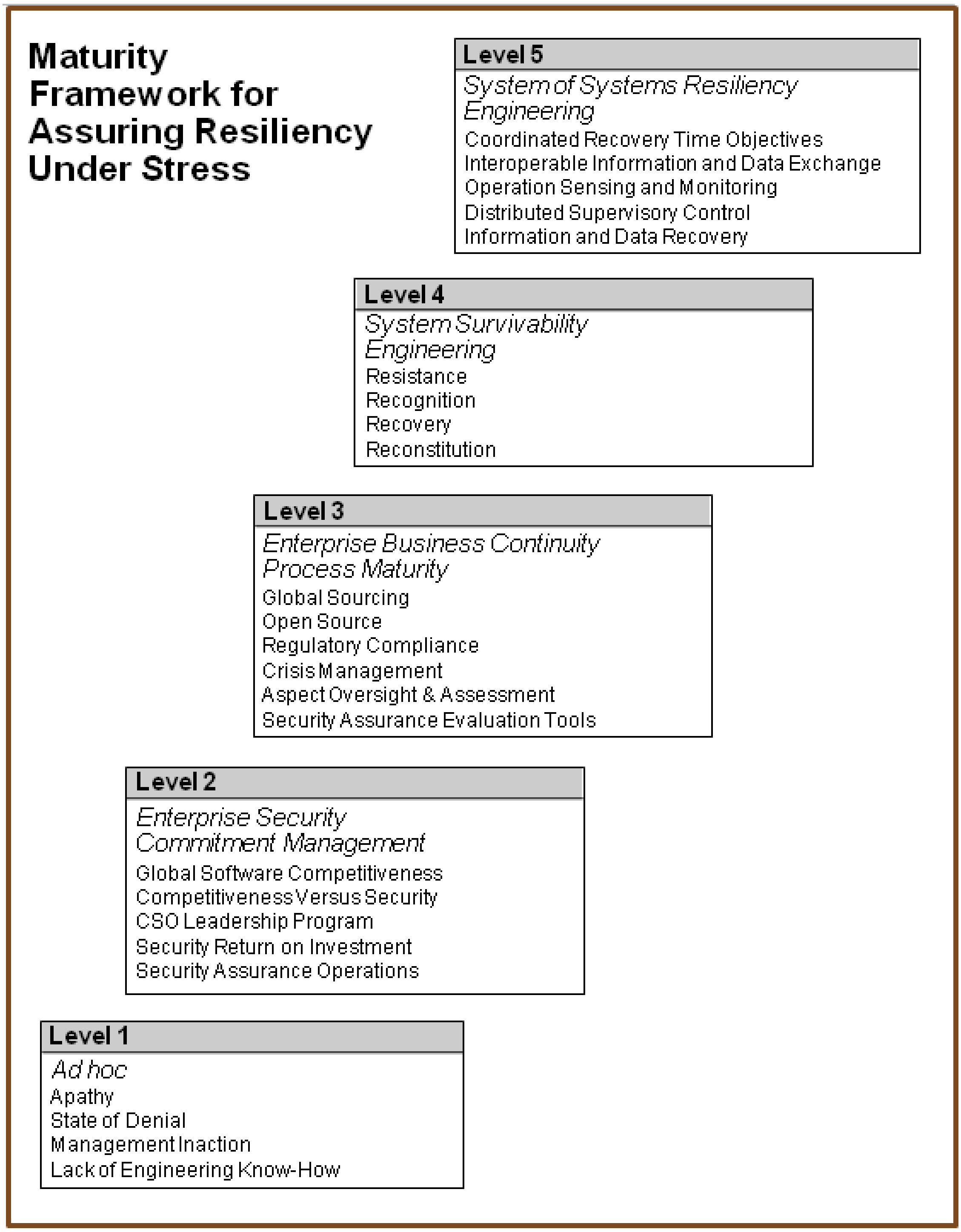
Level 4 System Survivability Engineering

- Goal: Demonstrate the achievement of system survivability through the management of faults and failures, sustainability processes, and RMA engineering.
- Focus Areas: Resistance, Recognition, Recovery, Reconstitution

Level 5 System of Systems Resiliency Engineering

- Goal: Demonstrate the achievement of system of systems resiliency through the management of external interactions and dependencies, the control of distributed supervisory processes, and the practice of next generation software engineering.
- Focus Areas: Coordinated Recovery Time Objectives, Interoperable Information and Data Exchange, Operation Sensing and Monitoring, Distributed Supervisory Control, Information and Data Recovery

Figure 4. Maturity framework



Maturity Framework for Assuring Resiliency Under Stress

Level 5
System of Systems Resiliency Engineering
Coordinated Recovery Time Objectives
Interoperable Information and Data Exchange
Operation Sensing and Monitoring
Distributed Supervisory Control
Information and Data Recovery

Level 4
System Survivability Engineering
Resistance
Recognition
Recovery
Reconstitution

Level 3
Enterprise Business Continuity Process Maturity
Global Sourcing
Open Source
Regulatory Compliance
Crisis Management
Aspect Oversight & Assessment
Security Assurance Evaluation Tools

Level 2
Enterprise Security Commitment Management
Global Software Competitiveness
Competitiveness Versus Security
CSO Leadership Program
Security Return on Investment
Security Assurance Operations

Level 1
Ad hoc
Apathy
State of Denial
Management Inaction
Lack of Engineering Know-How

Assurance provides justifiable confidence that software will function as intended. Assurance is demonstrated through model-based business, technical, and operational claims spanning management, process, and engineering arguments and model-based evidence (Table 1). An enterprise claiming to have achieved maturity in assuring enterprise resiliency under stress is expected to present correct and complete arguments that justify belief in the claim, along with clear and convincing evidence buttressing each argument.
The indicators shown under Focused Management Review, Defined Process Capability, and Designed Engineering Solution suggest the type of evidence sought for each level.

Table 1. Maturity Framework for Assuring Resiliency Under Stress goals and indicators

Maturity Framework for Assuring Resiliency Under Stress	Focused Management Review	Defined Process Capability	Designed Engineering Solution

Drive the business case and enterprise commitment towards the assurance of software security, business continuity, system survivability, and system of systems resiliency			
Level 2 Goal *Demonstrate commitment to security assurance through strategic management, internal processes, and defense in depth*	Competitiveness Versus Security Assessment and Tradeoff Security Return on Investment Incident Management	Chief Security Officer (CSO) Leadership Program Security Assurance Operations Configuration Management	Encryption Identity Management Access Control Authorization Management Accountability Management
Level 3 Goal *Demonstrate business continuity assurance through compliance management, external processes, and product engineering*	Regulatory Compliance Aspect Oversight & Assessment	Global Sourcing Risk Management Crisis Management	Open Source Commercial Off-the–Shelf Software Security Assurance Evaluation Tools
Level 4 Goal *Demonstrate the achievement of system survivability through the management of faults and failures, sustainability processes, and RMA engineering*	Incident Management Cyber Forensics Management of Defects, Faults, and Failures	Resistance Recognition Recovery Reconstitution	Reliability Engineering Availability Engineering Maintainability Engineering
Level 5 Goal *Demonstrate the achievement of system of systems resiliency through the management of external interactions and dependencies, the control of distributed supervisory processes, and the practice of next generation software engineering*	Coordinated Recovery Time Objectives Interoperability of Data and Information Exchange	Operation Sensing and Monitoring Distributed Supervisory Control Information and Data Recovery	Next Generation Software Engineering

Each of the levels is next explained in more detail.

Level 2: Enterprise Security Commitment Management

Goal: *Demonstrate commitment to security assurance through strategic management, internal processes, and defense in depth.*

How is commitment achieved, quantified, and expressed?

1. Commitment is achieved by coping with the stresses and conflicts between competitiveness and security.
2. Commitment is quantified by calculating security return on investment in terms of preparation and incident costs, cleanup costs, lost opportunity costs, and reconstitution cost.
3. Commitment is expressed through a CSO leadership program and security assurance operations.

Global Software Competitiveness

Global software competitiveness is a critical ingredient to the nation's prosperity centered on controlling scarce personnel resources, valued customers, fierce competitors, and chaotic event threats [COC 2002[36], COC 2007[37], GSCTool 2002[38], O'Neill 1998[39], Van Opstel 2007[40]]. However, there is an important national debate on competitiveness versus security centering on who pays the bill, the private or public sector.

It is the role of the chief security officer (CSO) to sort out this debate for the enterprise—to assess enterprise global software competitiveness, tradeoff competitiveness, and security [O'Neill 2004a[41], CompSecTool 2002[42]], determine the level of enterprise commitment to security assurance, and provide the security framework and capabilities to achieve assurance of cyberspace security readiness [NSQE Assess[43], Collins 2005[44], DHS 2006[45], CMMI 2006[46]].

In doing this, the CSO must draw upon business case models [O'Neill 2007a[47]], such as security return on investment [O'Neill 2007b[48], SecRoi Tool 2006[49]], to provide a basis for *rational action* to assist understanding, constructing, implementing, verifying, and overseeing the enterprise assurance of software trustworthiness and security. Further, the CSO must advance the assurance of software security by fully engaging enterprise executives, managers, and technical practitioners within the enterprise projects and functions in the assertion of assurance claims, the selection of validating arguments, and the collection of verifying evidence [Collins 2005[50]].

Focused Management Review

- Competitiveness Versus Security Assessment and Tradeoff
- Security Return on Investment
- Incident Management

Defined Process Capability

- Chief Security Officer (CSO) Leadership Program
- Security Assurance Operations
- Configuration Management

Designed Engineering Solution

- Encryption

[36] #dsy1016-BSI_COC02
[37] #dsy1016-BSI_COC07
[38] #dsy1016-BSI_gsc
[39] #dsy1016-BSI_O'Neill98
[40] #dsy1016-BSI_VanOp07
[41] #dsy1016-BSI_O'Neill04a
[42] #dsy1016-BSI_compsec
[43] #dsy1016-BSI_nsqe
[44] #dsy1016-BSI_Collins05
[45] #dsy1016-BSI_DHS06
[46] #dsy1016-BSI_CMMI06
[47] #dsy1016-BSI_ONeill07a
[48] #dsy1016-BSI_ONeill07b
[49] #dsy1016-BSI_secroi
[50] #dsy1016-BSI_Collins05

- Identity Management
- Access Control
- Authorization Management
- Accountability Management

Competitiveness Versus Security

There is an important national debate on cyber security [COC 2002[51]]. It centers on who pays the bill, the private or public sector. On the one hand, the public sector argues that security and competitiveness move together; therefore, the private sector should pay the cost to be competitive. On the other hand, the private sector argues that the Internet is public commons and enterprise security costs too much and the probability of occurrence of a significant cyber attack is too low to force the investment, especially during a period of economic recovery. While both are essential, it is clear that competitiveness and security travel on separate paths that do crisscross and overlap at certain points. The competitiveness versus security tradeoff may be tilted towards competitiveness, thereby exposing the nation's critical software infrastructure to predictable security threats. CIOs are invited to explore their competitiveness versus security tradeoffs by visiting the assessment tool at http://members.aol.com/ONeillDon2/comp-sec_frames.html [CompSecTool 2002[52]].

Security Return on Investment

With the dramatic increase in cyberspace incidents and perceptions about the high cost of investment for security readiness and survivability, there is a need for a method to reason about and compute security return on investment (ROI) [O’Neill 2007b[53]].

The availability of a common industry security ROI methodology would deliver numerous benefits. The contributors to security readiness, the costs to achieve security readiness, and the costs to recover from cyberspace incidents would be better understood. The enterprise could reason about its security investment decision with increased precision. The public-private collaboration discussion on who is responsible for paying for security would be better informed. The relationship between levels of security readiness and recovery costs would contribute to the actuarial basis for underwriting cyberspace insurance. The state of security readiness for the nation's critical infrastructure dependent on software could be better assessed.

Security return on investment is savings divided by cost. Reasoning about return on investment then is assisted by evaluating the expression [ROI: = savings/cost], where savings is cost avoidance resulting from resistance, recognition, and reconstitution efforts and cost includes preparation and incident cost. Incident cost is cleanup, lost opportunity, and critical infrastructure impact. CIOs and CSOs are invited to explore their security return on investment by visiting the assessment tool at http://members.aol.com/ONeillDon2/sec-roi_frames.html [SecROI Tool 2006[54]].

CSO Security Leadership Program

The chief security officer needs a security structure that packages the capabilities to achieve cyberspace security readiness into defined products and services. The security structure should meet several objectives, including clarifying costs, avoiding lawsuits, protecting the business, protecting the critical infrastructure, and controlling the disclosure of information (Figure 5). These objectives can be realized by systematically promoting awareness and obtaining commitment, conducting basic training in security practices, performing due diligence, ensuring the continuous operation of systems critical to the enterprise, and controlling the dissemination of information (Figure 5) [O’Neill 2003[55]].

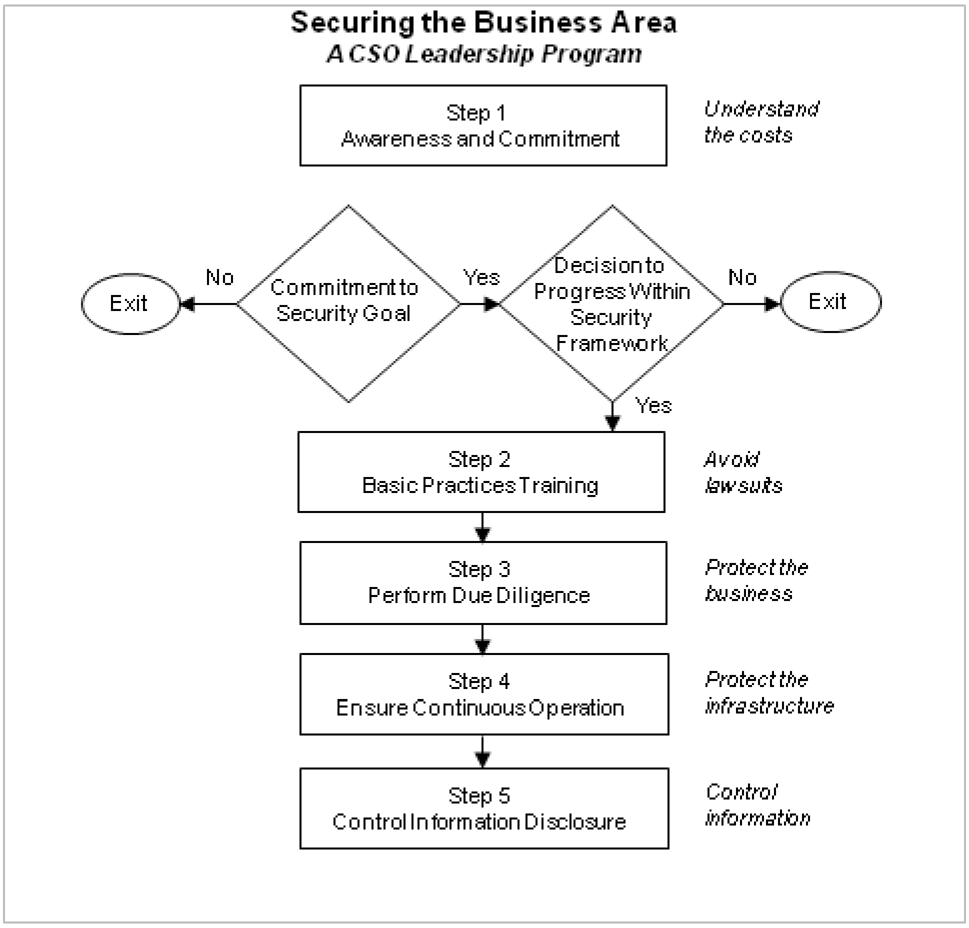
1. *Promote Awareness and Obtain Commitment* – Step 1 promotes awareness of security and elucidates the costs that underlie a commitment to achieve security. The business area is asked if it is prepared to make a commitment to the goal to be free of cyberspace intrusion. Business areas that choose to

[51] #dsy1016-BSI_COC02
[52] #dsy1016-BSI_compsec
[53] #dsy1016-BSI_ONeill07b
[54] #dsy1016-BSI_secroi
[55] #dsy1016-BSI_O’Neill03

make the commitment to being secure are asked if they would like to progress within the security framework. Those not making the commitment to security or choosing not to progress within the security framework conduct management presentations to discuss these decisions.

2. *Conduct Basic Security Practices Training* – Step 2 seeks to spike lawsuits by training enterprise staff in security best practices. All employees are introduced to the culture of security and the techniques and practices for resisting cyberspace intrusion. Architects, designers, and lead personnel are further introduced to the technology and practices for recognizing the presence of a cyberspace intrusion. Architects and senior personnel then participate in an intensive workshop on reconstitution and survivability that will lead to a secure architecture for the critical assets of the business area.
3. *Perform Due Diligence* – Step 3 seeks to protect the business by performing due diligence through the implementation of resistance and recognition techniques and practices. This entails the sacrifice of certain cost effectiveness practices that enhance competitiveness at the expense of security.
4. *Ensure Continuous Operation* – Step 4 is aimed at protecting the critical infrastructure by ensuring the continuous operation of critical assets through the implementation of reconstitution and recovery. This involves the sacrifice of certain architectural techniques and change tolerance practices that enhance competitiveness at the expense of security.
5. *Control the Disclosure of Information* – Step 5 seeks to control the disclosure of information through selective sharing and hiding of security vulnerabilities, intrusion incidents, security practices and technology, and critical domain knowledge. Hiding operations apply to intruders, the competition, and anyone without the need to know.

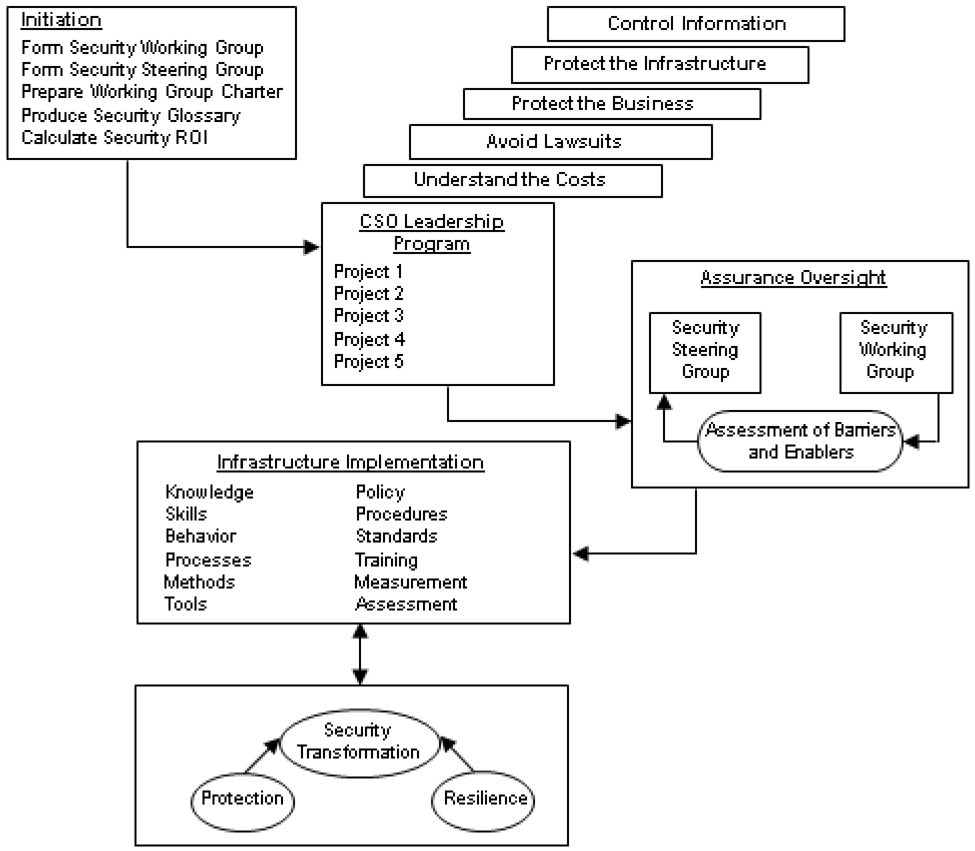
Figure 5. CSO Leadership Program



Security Assurance Operations

Software security assurance operations and their interactions are illustrated in Figure 6.

Figure 6. Security assurance operations



Configuration Management

Software changes are a source of cyber security vulnerability. Whether correcting defects from program test reports or handling software change requests from customers or users, a change must be dispositioned and a release must be planned and implemented. Each step is accompanied by management and technical reviews. The result is a user installed release that occurs at some release frequency. Figure 7 presents the software change management process as an Entry, Task, Verification, and Exit (ETVX) diagram. Figure 8 presents the software change management process as an operational flow.

Figure 7. Software Change Management ETVX Diagram

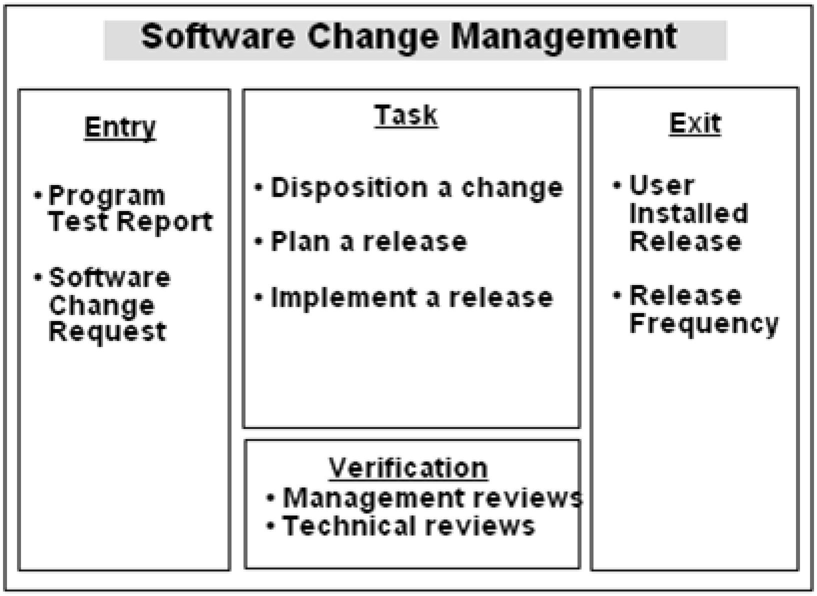
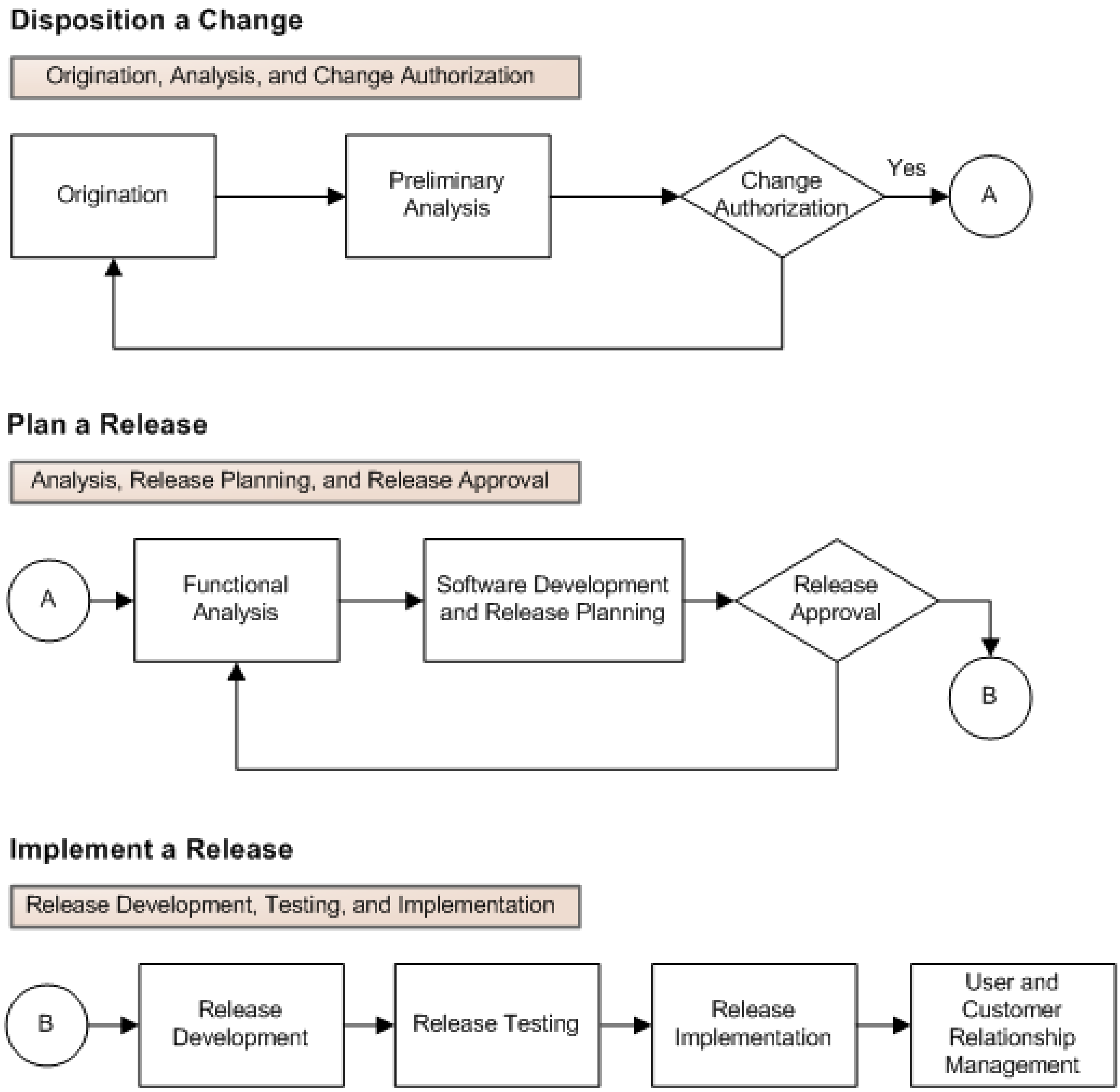


Figure. 8. Software change management operational flow


Disposition a Change
Origination, Analysis, and Change Authorization
Origination
Preliminary Analysis
Change Authorization
Yes
A
Plan a Release
Analysis, Release Planning, and Release Approval
A
Functional Analysis
Software Development and Release Planning
Release Approval
B
Implement a Release
Release Development, Testing, and Implementation
B
Release Development
Release Testing
Release Implementation
User and Customer Relationship Management

Level 3: Enterprise Business Continuity Process Maturity

Goal: *Demonstrate business continuity assurance through compliance management, external processes, and product engineering.*

How is business continuity achieved?

1. Business continuity begins by focusing on supply chain management, including global sourcing and open source.
2. It extends to regulatory compliance and aspect oversight and assessment.
3. Business continuity culminates in the systematic crisis management steps of prevention and response that sustain stability or result in a return to stability.

External factors impacting business continuity include global sourcing, open source, and regulatory compliance [Caralli 2006[56]]. Offshore outsourcing is an asymmetric tactic that delivers a competitive

[56] #dsy1016-BSI_Caralli06

advantage increasingly used to achieve competitiveness on the cheap, but due diligence is needed in the organization and oversight of responsibilities and services if success is to be achieved and risks contained [O'Neill 2004b[57]]. Open source is a commodity product by definition, and the evaluation of open source versus closed source is considered security neutral despite drivers on both sides. Regulatory demands of all kinds are increasing and cut a wide swath from financial management to security assurance, with information technology aspects serving as both the target of regulation and the means to demonstrate compliance [Baker 2008[58]].

Beginning with an unstable situation, crisis management comprises the systematic steps of prevention and response that sustain stability or that result in a return to stability. Verifying the enterprise assurance of software trustworthiness and security [Collins 2005[59]] is achieved through demonstration and assessment, including industry state of the art and state of the practice, enterprise assessment of assurance infrastructure, enterprise assessment of technical foundations, and demonstration of enterprise survivability and resilience.

Focused Management Review

- Regulatory Compliance
- Aspect Oversight & Assessment

Defined Process Capability

- Global Sourcing
- Risk Management
- Crisis Management

Designed Engineering Solution

- Open Source
- Commercial Off-the–Shelf Software
- Security Assurance Evaluation Tools

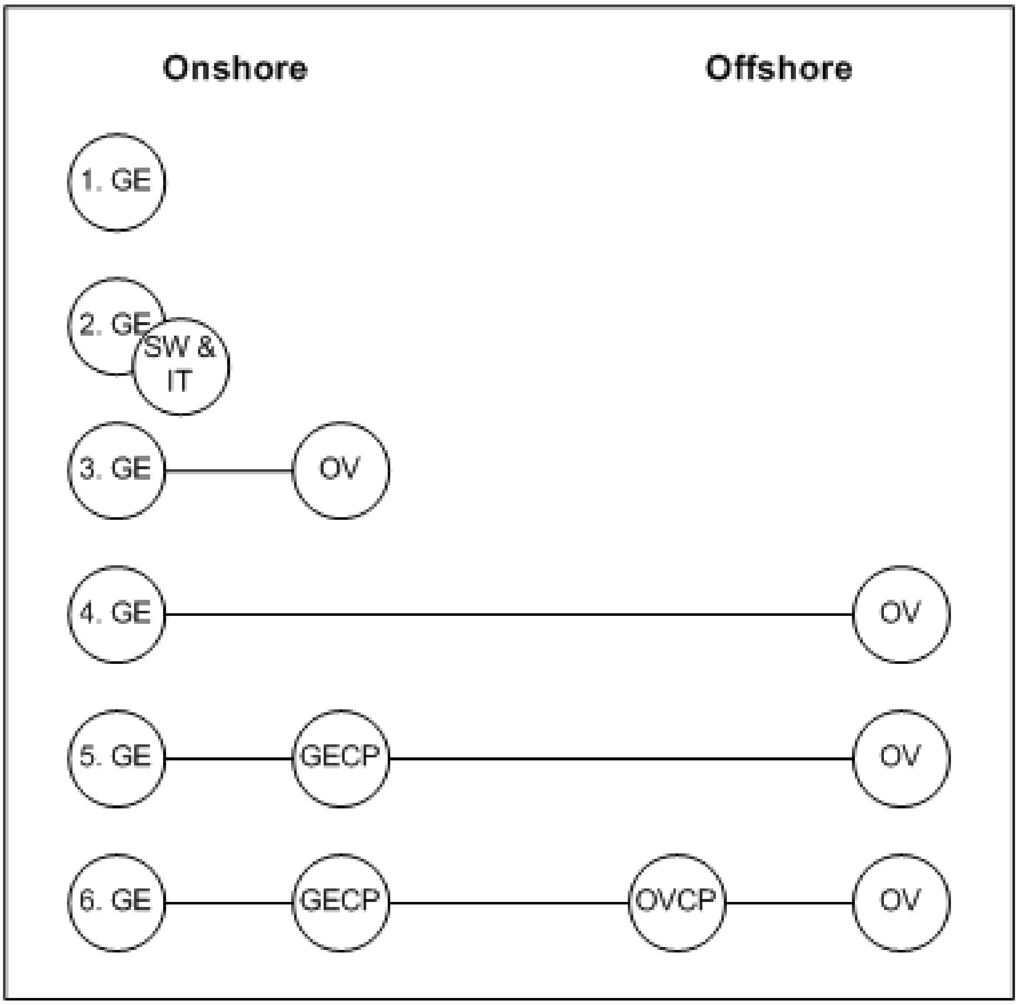
Global Sourcing

Studies on global software competitiveness conducted by the Center for National Software Studies reveal that offshore outsourcing is an asymmetric tactic that delivers a competitive advantage [O'Neill 2004b[60]]. As global enterprises increasingly seek to achieve competitiveness on the cheap, global outsourcing is becoming more widespread. But due diligence is needed if success is to be achieved. What should global enterprises look for in an outsourcing partner?

An innovation in the outsourcing space [USPTO 2004[61]] capable of managing to scale the initiation of global enterprise projects both large and small and their fulfillment by offshore vendors also provides a framework to assure software security. Driven by skills, cost, commoditization, innovation, risk, and scale considerations, the innovation disassembles the supply chain of the software project life cycle and repackages the defined processes, practices, and capabilities, including their underlying knowledge, skills, and behaviors, into a pipeline of managed and controlled onshore and offshore nodes of repeatable services whose arrangement is adaptable in striking the right balance and fit among the drivers. Disassembling and repackaging software and information technology has progressed through stages characterized as follows (Figure 9:

Figure 9. Disassembling and Repackaging Software

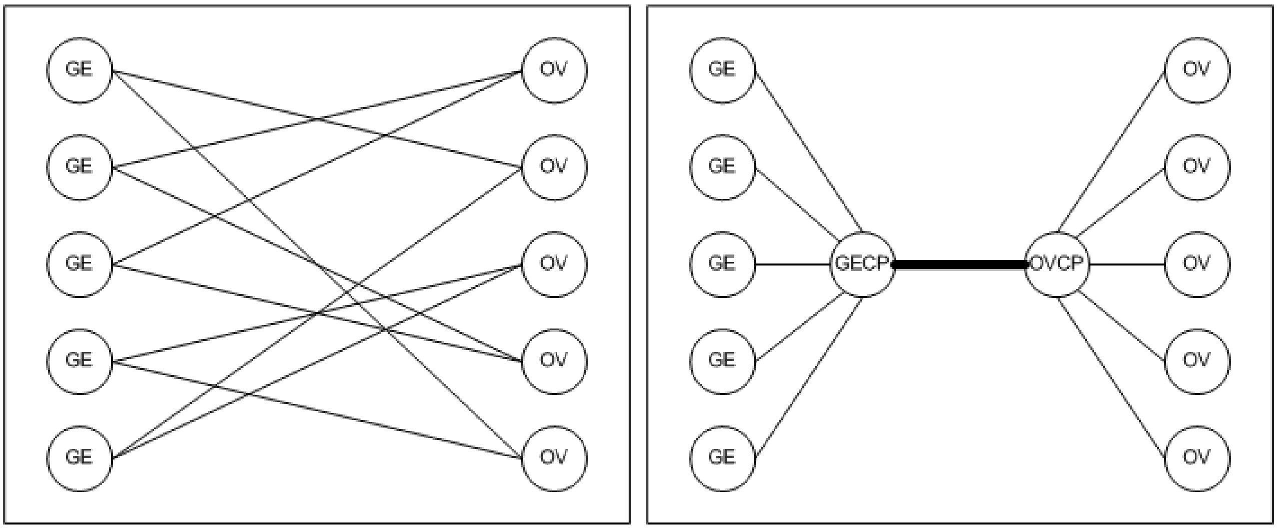
[57] #dsy1016-BSI_ONeill04b
[58] #dsy1016-BSI_Baker08
[59] #dsy1016-BSI_Collins05
[60] #dsy1016-BSI_ONeill04b
[61] #dsy1016-BSI_USPTO04



1. Software and IT integral to using departments of a global enterprise
2. Functionalizing software and IT as an in-house operation driven by skills
3. Functionalizing software and IT as an outsourced onshore vendor operation driven by skills and cost
4. Functionalizing software and IT as an outsourced offshore vendor operation driven skills, cost, and commoditization
5. Further functionalizing the administration of the offshore outsourcing operation as an outsourced onshore control point driven by skills, cost, commoditization, innovation, and risk
6. Splitting the offshore outsourced operation into onshore and offshore control points driven by skills, cost, commoditization, innovation, risk, and scale

Offshore outsourcing is becoming increasingly pervasive (Figure 10). In order to accommodate the increasing scale of offshore outsourcing both within an enterprise and across various industry sectors, an offshore outsourcing architecture is used to reduce complexity by disassembling and repackaging functions and information flow (Figure 11).

Figure 10. Network complexity unrestrained **Figure 11. Network complexity managed**



The inside track to offshore outsourcing features a Trusted Pipe™ staffed with intelligent middlemen. The Trusted Pipe™ is a multidimensional channel capable of exchanging essential management, engineering, process, business, legal, and cultural messages in a predictable and reliable manner. Intelligent middlemen are trained to compose and understand these messages using a comprehensive and robust training program that delivers the knowledge, skills, and behaviors for managing across borders and cultures.

®Trusted Pipe is registered with U.S. Patent and Trademark Office by Don O'Neill.

Open Source

Open source is a commodity product by definition. Open source refers to a computer program whose source code is made available to the public for modification or improvement as individual users desire. In addition, open source is ordinarily accompanied by a license that requires users to maintain the program as open source. Interestingly, major suppliers like IBM and Microsoft are moving to the middle away from the proprietary model for certain product categories. These suppliers, however, retain a stake in the open source repository. For example, IBM dedicates 600 programmers to sustaining the Linux open source. In part the open source movement is market driven; in part suppliers are conceding commoditization for part of the product stack.

Open source evolution is driven by users who submit changes. These changes are not simply change requests in the form of requirements or hoped for capabilities; instead they are the very source code implementation of the change a user hopes to see adopted by the community. In the past four years, there have been 38,000 changes delivered by 1,000 contributors, where 20 contributors have authored 50% of the changes [O’Neill 2006a[62]].

The evaluation of open source versus closed source is considered security neutral despite drivers on both sides. Open source is available to potential hackers, but open source is also under continuous peer review and inspection by a diverse audience. Open source quality is assisted by many practitioners inspecting source code components and rapid correction and dissemination of corrections. While support is generally available within the community of users, there is a lack of accountability. The total cost of ownership (TCO) is situational. While the open source is free and licensed, a user must incur hardware, other software, training, conversion, and other support costs. In addition, due diligence requires a user to field a staff knowledgeable in the open source code base used. Underlying the cost attractiveness of open source is that there is a zero marginal cost of scale because open source doesn't require additional licenses as an installation grows.

Crisis Management

A crisis is an unstable situation. Crisis management comprises the systematic steps of prevention and response that sustain stability or that result in a return to stability. Crisis management starts with crisis

[62] #dsy1016-BSI_ONeill06a

prevention, which spans identifying a crisis, planning a response to the crisis, and confronting the crisis. Crisis management concludes with crisis response and resolution, which ideally involves executing a plan for an identified crisis. Certain preliminary measures need to be taken to prevent a crisis. Certainly the enterprise should plan ahead, project likely outcomes, and avoid decisions that have the potential to trigger a crisis.

While crisis management builds on risk management, its focus is different in one important respect. Using risk management, a potential risk might be identified and risk resolution might determine to do nothing based on a low-probability, high-cost argument. In choosing avoidance over sustainment, an organization may find itself depending on risk management to contemplate the probability of one event or another with their propagation effects but without planning and providing for the recovery and switchover capabilities needed to ensure continuous operation. Managing risk to avoid a risk event produces outcomes different from planning on withstanding the occurrence of the risk event and what comes next. Crisis management utilizes the risk management process but then presses forward to the stages of response and resolution.

Level 4: System Survivability Engineering

Goal: *Demonstrate the achievement of system survivability through the management of faults and failures, sustainability processes, and RMA engineering.*

Survivability spans the resistance to cyber attack, the recognition of a cyber attack, and the reconstitution of enterprise software operations following a cyber threat or cyber attack [Ellison 1997[63], Linger 2001[64]]. The Software Engineering Institute defined survivability “as the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.”

The Software Engineering Institute identifies the key properties of survivable systems as resistance to attacks, recognition of attacks and the extent of damage, recovery of full and essential service after attack, and adaptation and evolution to reduce effectiveness of future attacks. Survivability is achieved through the right blend of function, form, and fit. Software practices that result in highly secure and survivable software products may benefit security at the expense of competitiveness.

Focused Management Review

- Incident Management
- Cyber Forensics
- Management of Defects, Faults, and Failures

Defined Process Capability

- Resistance
- Recognition
- Recovery
- Reconstitution

Designed Engineering Solution

- Reliability Engineering
- Availability Engineering
- Maintainability Engineering

Recovery and Reconstitution

The steps to reconstitute critical software operations center on the technology for ensuring continuous operations, backing up, switching over, and restarting critical operations.

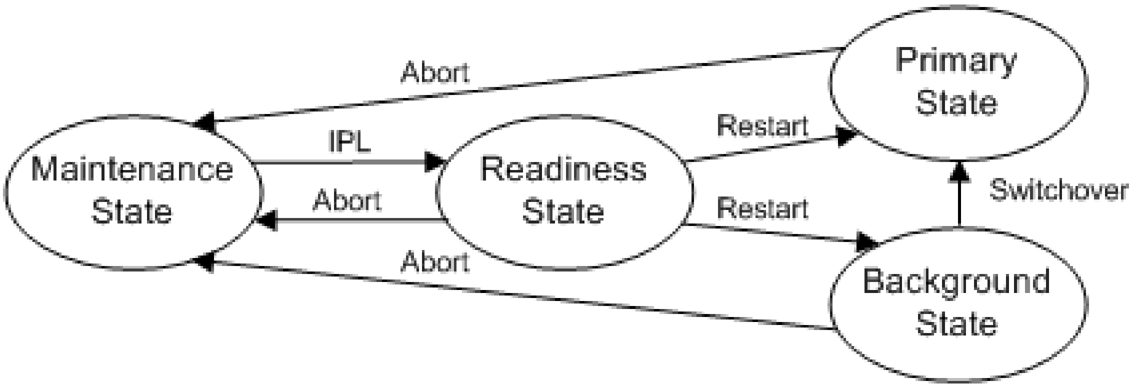
Threats to the survivability of software operations begin with the natural and man-made threats to physical plant, electrical supply, and telecommunications connectivity used by critical software operations. The user of these assets must anticipate and recognize the loss of assets and provide for the reconstitution of the

[63] #dsy1016-BSI_Ellison97
[64] #dsy1016-BSI_Linger01

operation. The owner of the critical software system must resist threats, recognize attacks, and provide for the reconstitution of the operation.

Whether the threat is natural or man-made, physical or logical, there is the need to provide for the reconstitution of the operation. A critical software operation whose continuous operation must be assured needs a disaster recovery plan spanning computing equipment, connectivity, software, and operating personnel, along with the transition mechanisms to carry it out (Figure 12).

Figure 12. Recovery state transitions



Level 5: System of Systems Resiliency Engineering

Goal: *Demonstrate the achievement of system of systems resiliency through the management of external interactions and dependencies, the control of distributed supervisory processes, and the practice of next generation software engineering.*

In order to achieve resilience in the nation's critical infrastructure, three levels of continuity must be assured: high availability, continuous operation, and disaster recovery. These must span servers, storage, software and automation, networking and infrastructure, and skills and services. If security is not simply to be bolted on but is instead to be built in, there must be a harmonious correspondence and alignment between security solutions and software systems architectures.

Focused Management Review

- Coordinated Recovery Time Objectives
- Interoperability of Data and Information Exchange

Defined Process Capability

- Operation Sensing and Monitoring
- Distributed Supervisory Control
- Information and Data Recovery

Designed Engineering Solution

- Next Generation Software Engineering

Next Generation Software Engineering

Next generation software engineering involves obtaining intellectual control over systems and exerting operational control over systems of systems being developed, fielded, and operated [Caralli 2006[66], Caralli 2007[67], CNSS 2005[68], DACS 2006[69]]. Without such understanding, the responsibilities of enterprise

[66] #dsy1016-BSI_Caralli06
[67] #dsy1016-BSI_Caralli07
[68] #dsy1016-BSI_CNSS05
[69] #dsy1016-BSI_DACS06

governance over information systems operations and the data they produce cannot be dependably exercised with any degree of confidence.

1. Those who develop systems must obtain intellectual control through completeness, correctness, and consistency arguments buttressed by the aspects of rules of construction, multiple views, and technology attributes.
2. Those who field systems of systems must exert operational control through coordinated recovery time objectives, interoperability, and distributed supervisor control.
3. Those who operate systems and systems of systems must actuate operational control in achieving business continuity.

Security professionals are expected to employ next generation software engineering modeling technology to interpret the cross product of the computing state and the threat environment in identifying the distributed supervisory control protocols whose actuation ensures the least mitigation necessary to impede these effects.

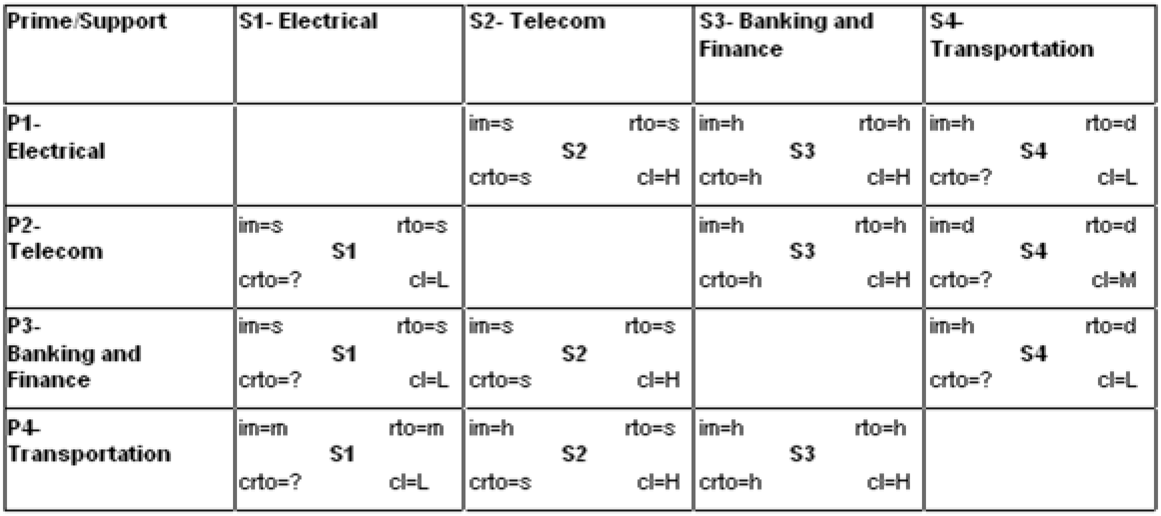
Coordinated Recovery Time Objectives

When we look at the nation's critical infrastructure industry sectors, none of them has the defenses to combat the intersection of a neglectful software industry with its vulnerabilities and a determined, innovative bad actor intent on launching cyber security exploits. The lack of strategic coordination among these industry sectors and especially the absence of coordinated recovery time objectives [O’Neill 2006b[70]] may be setting the stage for a coordinated cyber and physical attack.

For each critical infrastructure sector, under what circumstances of use are dependent sectors not available? Non-available is defined in a specific situation description. For each instance of non-availability, what is the immediacy of need (im) and the required recovery time objective (rrto) for each? These are expressed in seconds (s), minutes (m), hours (h), days (d), and weeks (w).

Canonical verification of the statement of critical infrastructure sector dependency is governed by the degree of correspondence where recovery time objectives (rto) are established in relationship to immediacy of need (im). Shortfall reveals technical and management feasibility and state of the practice issues. Operational verification of the statement of critical infrastructure sector dependency is governed by the degree to which the recovery time objective (rto) has been coordinated among the prime and support sectors in arriving at a coordinated recovery time objective (crto). Shortfall reveals issues in stovepipe culture, management will, and regulatory environment. A confidence level is assigned to the outcome in terms of high (H), medium (M), or low (L). See Table 2.

Table 2. Recovery time objectives



Prime/Support	S1- Electrical	S2- Telecom	S3- Banking and Finance	S4- Transportation

P1- Electrical		im=s rto=s
		S2
		crto=s cl=H
			im=h rto=h
			S3
			crto=h cl=H
				im=h rto=d
				S4
				crto=? cl=L

P2- Telecom	im=s rto=s
	S1
	crto=? cl=L
			im=h rto=h
			S3
			crto=h cl=H
				im=d rto=d
				S4
				crto=? cl=M

P3- Banking and Finance	im=s rto=s
	S1
	crto=? cl=L
		im=s rto=s
		S2
		crto=s cl=H
				im=h rto=d
				S4
				crto=? cl=L

P4- Transportation	im=m rto=m
	S1
	crto=? cl=L
		im=h rto=s
		S2
		crto=s cl=H
			im=h rto=h
			S3
			crto=h cl=H	

[70] #dsy1016-BSI_ONeill06b

Notes:

1. To learn how well the sector supports other sectors, read down.
2. To learn how well the sector is supported by other sectors, read across.

Process for producing a statement of dependency:

1. Identify prime activities.
2. Identify supporting dependent activities.
3. Determine the immediacy of need for each supporting dependent activity relative to each prime activity it supports. Note that these results may vary for a given dependent activity.
4. Determine the likely required recovery time objective for each supporting dependent activity relative to each prime activity it supports.
5. Verify that the immediacy of need and required recovery time objective are consistent. Where they are not consistent, enter the inconsistency on the issues list.
6. Determine the coordinated recovery time objective for each supporting dependent activity relative to each prime activity it supports.
7. Verify that the required recovery time objective and coordinated recovery time objective are consistent. Where they are not consistent, enter the inconsistency on the issues list.
8. Assign a confidence level for each supporting dependent activity relative to each prime activity its supports based on the confidence in the level of commitment in the coordinated recovery time objective and an assessment of the realism of the immediacy of need.
9. Review issues list.
10. Review entries assigned low confidence level.

Operation Sensing and Monitoring

It is thought that systems of systems, unlike systems whose behavior is more deterministic, may be subject to progressive, propagating, and cascading failures. Understanding the triggering events and speed of such events is the prerequisite to establishing the necessary operational control [Phoha 2006[71]].

Distributed Supervisory Control

If the critical infrastructure is to be resilient, its sector managers and systems must respond to guidance from intelligent middlemen whose influence is felt before, during, and after a crisis. This guidance is informed by ongoing operation sensing and monitoring.

Each intelligent middleman possesses the broad range of hard and soft skills spanning the cultural, ethical, legal, business, process, management, and engineering dimensions needed to meet the challenges of the critical infrastructure as a system of systems in anticipating, avoiding, minimizing, withstanding, and recovering from crosscutting effects and to impede the emergence of propagating and cascading effects.

Intelligent middlemen are expected to employ next generation software engineering modeling technology to interpret the cross product of the computing state and the threat environment in identifying the distributed supervisory control protocols whose actuation ensures the least mitigation necessary to impede these effects.

Information and Data Recovery

Hierarchical storage management of information spans disk, optical, and tape media. Multinode topologies like dual-site and three-site mega centers are structured as distributed architectures designed to accommodate the mirroring and replication of data from which rapid and automatic recovery are accomplished.

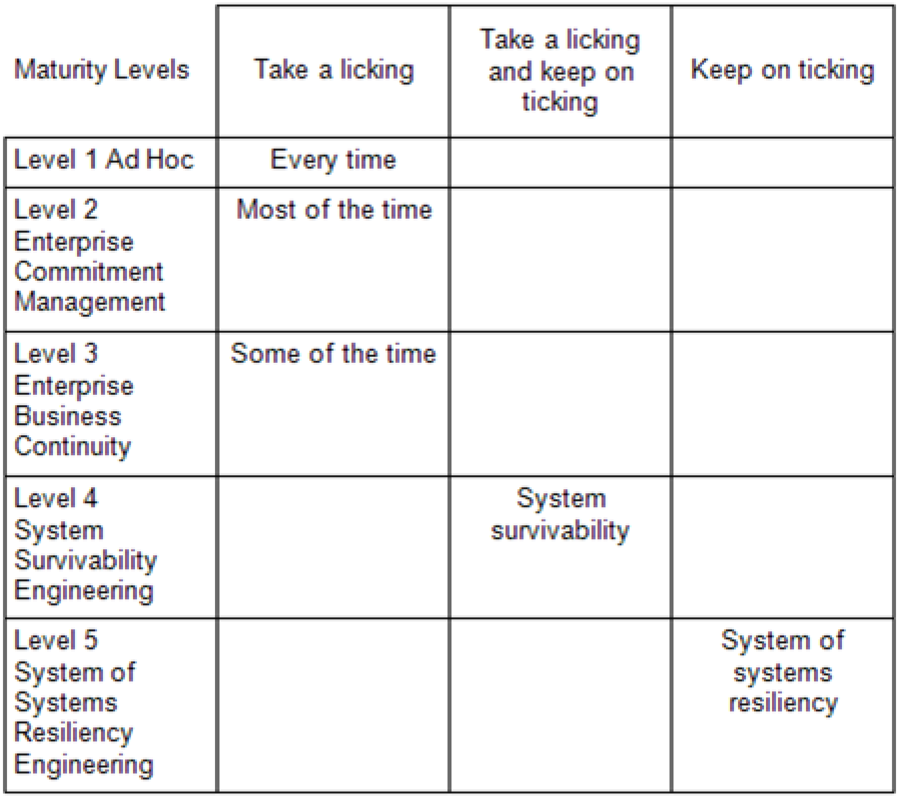
[71] #dsy1016-BSI_Phoha06

Summary

One respected researcher seemed to concede the high ground of resiliency, that is, avoidance, in associating resiliency with the Timex slogan, “Take a licking and keep on ticking” [Perelman 2006[72]]. In Table 3 the Timex slogan is parsed by maturity level.

1. The payoff in the early levels is progressively reduced cleanup cost, lost opportunity costs, and reconstitution costs through improved ability to recognize, withstand, and minimize vulnerabilities and attacks.
2. The payoff at level 4 is the resumption of service for a system through improved ability to recover.
3. The payoff at level 5 is the elimination of crosscutting impacts propagated from other systems through improved ability to avoid and anticipate adversity.

Table 3. Take a licking and keep on ticking



Maturity Levels	Take a licking	Take a licking and keep on ticking	Keep on ticking
Level 1 Ad Hoc	Every time		
Level 2 Enterprise Commitment Management	Most of the time		
Level 3 Enterprise Business Continuity	Some of the time		
Level 4 System Survivability Engineering		System survivability	
Level 5 System of Systems Resiliency Engineering			System of systems resiliency

Evidence-Based Assurance Assessment

The specification of a framework for assuring the resiliency of the critical infrastructure through a management, process, and engineering framework of capabilities and solutions is now complete. We are ready to consider the model-based business, technical, and operational claims, arguments, and evidence needed for evidence-based assurance assessment. An enterprise claiming to have achieved maturity in assuring enterprise resiliency under stress is expected to present correct and complete arguments that justify belief in the claim, along with clear and convincing evidence buttressing each argument.

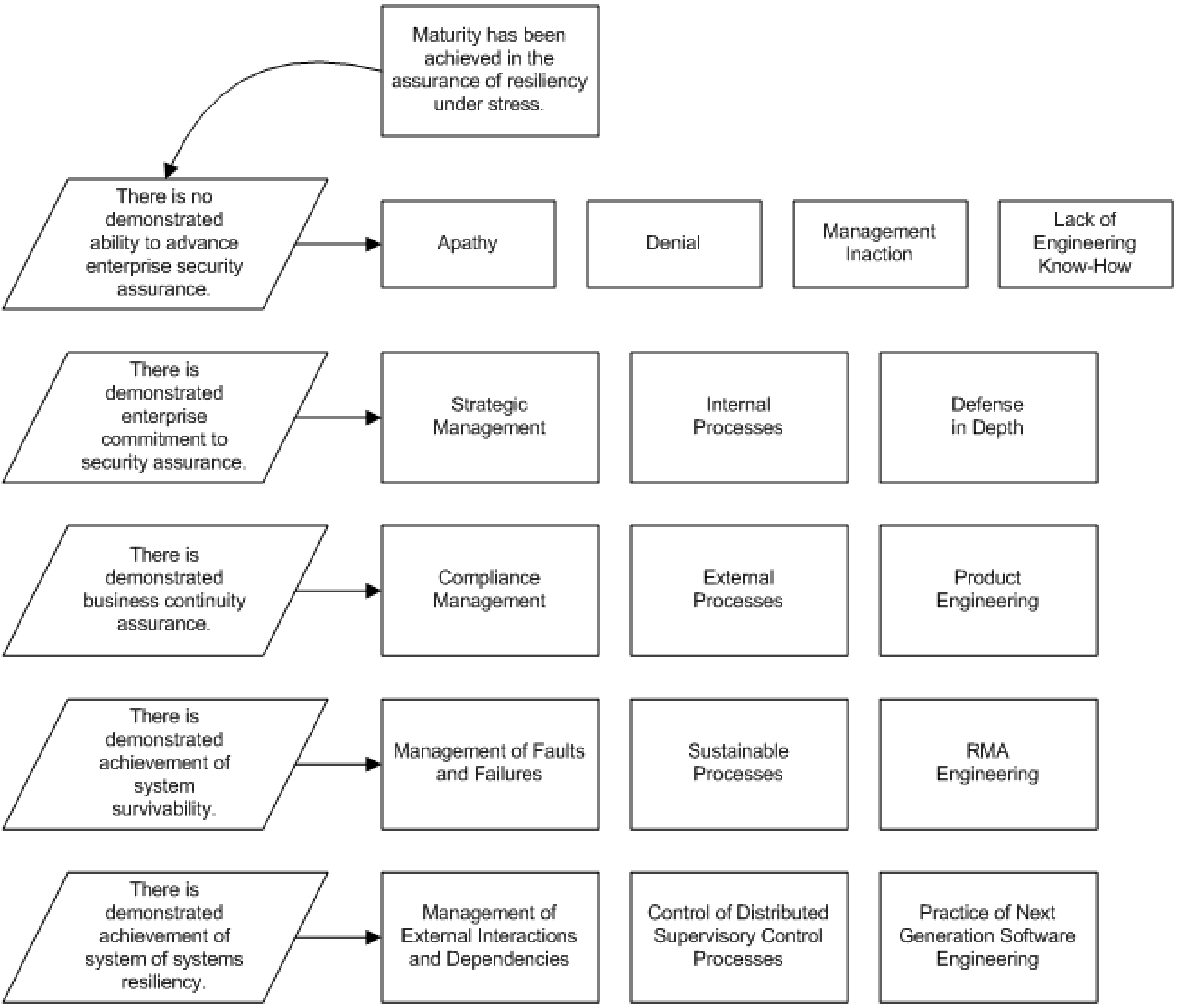
The purpose of Assurance Assertion Management (AAM) is to reason about the emergent properties of large, complex software-intensive systems, to take action to steer enterprise commitment towards their assurance, and to guide buyers, users, and the public in setting their level of confidence in these systems and systems of systems. An assurance assertion is a statement that inspires confidence. Assurance assertions are useful in assisting reasoning about the emergent properties of large, complex software-intensive systems. These product properties transcend the rigorous and precise methods of assessing essential compliance

[72] #dsy1016-BSI_Perel06

beyond those used in process conformance and product testing [Goodenough 2007[73]]. Some attribute and aspect examples of emergent properties associated with software products, systems, and systems of systems include safety, security, resiliency, privacy, and trustworthiness [Jackson 2007[74]].

The assurance claim for resilience assurance, the five arguments from the resiliency assurance framework, and the types of evidence expected for each argument are shown in Figure 13.

Figure 13. Evidence-based assurance assessment



Maturity has been achieved in the assurance of resiliency under stress.
There is no demonstrated ability to advance enterprise security assurance.
Apathy
Denial
Management Inaction
Lack of Engineering Know-How
There is demonstrated enterprise commitment to security assurance.
Strategic Management
Internal Processes
Defense in Depth
There is demonstrated business continuity assurance.
Compliance Management
External Processes
Product Engineering
There is demonstrated achievement of system survivability.
Management of Faults and Failures
Sustainable Processes
RMA Engineering
There is demonstrated achievement of system of systems resiliency.
Management of External Interactions and Dependencies
Control of Distributed Supervisory Control Processes
Practice of Next Generation Software Engineering

The assessment questions in Appendix A provide the basis for collecting the evidence-based assurance needed to verify the arguments and determine compliance. Assurance assertions themselves are subject to validation and verification. The claim-argument segment of the assurance assertion chain is validated when the correspondence between a claim and its arguments is shown to be clear and convincing with respect to completeness and correctness. The argument-evidence segment of the assurance assertion chain is verified according to the degree of correspondence between the evidence and the argument (Table 4).

Four levels of confidence for appraising evidence are identified as follows:

1. The evidence in support of the argument is insufficient.
2. The preponderance of the evidence supports the argument, e.g., through assessment, interviews, testimony, and inspection.

[73] #dsy1016-BSI_Good07

[74] #dsy1016-BSI_Jackson07

3. The evidence in support of the argument is clear and convincing, e.g., measurement and static analysis.
4. The evidence in support of the argument is beyond the shadow of a doubt, e.g., demonstration and dynamic analysis.

Table 4. Claim, arguments, and evidence

Claim	Arguments	Evidence
Maturity achieved in the assurance of enterprise resilience under stress.		
	1. Demonstrated inability to advance enterprise security assurance	1.1 Exhibiting evidence of apathy 1.2 Exhibiting evidence of denial 1.3 Exhibiting evidence of management inaction 1.4 Exhibiting evidence of lack if engineering know-how
	2. Demonstrated enterprise commitment to security assurance through strategic management, internal processes, and defense in depth	2.1 Conducted global software competitiveness assessment 2.2 Conducted competitiveness versus security tradeoff 2.3 Calculated security return on investment 2.4 Established chief security officer (CSO) leadership program 2.5 Instituted security assurance operations infrastructure 2.6 Utilized configuration management 2.7 Utilized encryption 2.8 Utilized identity management 2.9 Utilized access control 2.10 Utilized authorization management 2.11 Utilized accountability management
	3. Demonstrated business continuity assurance through compliance management, external processes, and product engineering	3.1 Managed regulatory compliance 3.2 Conducted aspect oversight and assessment 3.3 Managed global sourcing 3.4 Managed risk 3.5 Managed crisis management readiness 3.6 Managed open source

		3.7 Managed commercial off-the-shelf software 3.8 Utilized security assurance evaluation tools
	4. Demonstrated the achievement of system survivability through the management of faults and failures, sustainability processes, and RMA engineering	4.1 Managed incidents 4.2 Monitored cyber forensics 4.3 Managed defects, faults, and failures 4.4 Engineered resistance 4.5 Engineered recognition 4.6 Engineered recovery 4.7 Engineered reconstitution 4.8 Performed reliability engineering 4.9 Performed availability engineering 4.10 Performed maintainability engineering
	5. Demonstrated the achievement of system of systems resiliency through the management of external interactions and dependencies, the control of distributed supervisory control processes, and the practice of next generation software engineering	5.1 Coordinated recovery time objectives 5.2 Coordinated interoperability of data and information exchange 5.3 Applied operation sensing and monitoring 5.4 Applied distributed supervisory control 5.5 Applied information and data recovery 5.6 Exploited next generation software engineering

Appendix: Resiliency Assurance Assessment Questions

A- Transparent assessment of commitment

1. Is there a demonstrated inability to advance enterprise security assurance?

1.1 Has no evidence of apathy through interview questions and answers been exhibited?

1.2 Has no evidence of denial through interview questions and answers been exhibited?

1.3 Has no evidence of management inaction through interview questions and answers been exhibited?

1.4 Has no evidence of lack of engineering know-how through interview questions and answers been exhibited?

B- Commoditized protection

2. Is there a demonstrated enterprise commitment to security assurance through strategic management, internal processes, and defense in depth?

2.1 Has a global software competitiveness assessment been conducted using criteria and questions resulting in findings and recommendations?

2.2 Has a competitiveness versus security tradeoff been conducted using criteria resulting in findings?

2.3 Has a security return on investment with input parameters and computed result for initial determination and verification through actual results been conducted?

2.4 Has a chief security officer (CSO) leadership program been established with explicit commitments, training, and defined activities?

2.5 Has a security assurance operations infrastructure with initiation, process enactment, and oversight artifacts been instituted?

2.6 Is configuration management with traceability to changes utilized?

2.7 Is encryption utilized?

2.8 Is identity management utilized?

2.9 Is access control utilized?

2.10 Is authorization management utilized?

2.11 Is accountability management utilized?

C- Audited process

3. Is there demonstrated business continuity assurance through compliance management, external processes, and product engineering?

3.1 Is regulatory compliance for specified policies managed?

3.2 Is aspect oversight and assessment for specified attributes conducted?

3.3 Is global sourcing for each node in the supply chain and its management, process, and engineering aspects managed?

3.4 Is risk of management, process, and engineering aspects managed?

3.5 Are crisis management readiness exercises spanning people, process, technology infrastructure, connectivity, and interoperability for the enterprise and its dependent partners managed?

3.6 Are open source trustworthiness and security aspects managed?

3.7 Are commercial off-the-shelf software trustworthiness and security aspects managed?

3.8 Are security assurance evaluation tools for legacy software, new development, outsourced, open source, and commercial off-the-shelf software utilized?

D- Certified engineering

4. Is there demonstrated achievement of system survivability through the management of faults and failures, sustainability processes, and RMA engineering?

4.1 Are incidents managed?

4.2 Are cyber forensics monitored?

4.3 Are defects, faults, and failures managed?

4.4 Is resistance engineered?

4.5 Is recognition engineered?

4.6 Is recovery engineered?

4.7 Is reconstitution engineered?

4.8 Is reliability engineering performed?

4.9 Is availability engineering performed?

4.10 Is maintainability engineering performed?

E- Research and engineering

5. Is there demonstrated achievement of system of systems resiliency through the management of external interactions and dependencies, the control of distributed supervisory control processes, and the practice of next generation software engineering?

5.1 Are recovery time objectives coordinated?

5.2 Is interoperability of data and information exchange coordinated?

5.3 Is operation sensing and monitoring applied?

5.4 Is distributed supervisory control applied?

5.5 Is information and data recovery applied?

5.6 Is next generation software engineering exploited?

Tools

[CompSecTool 2002] O’Neill, Don, “Competitiveness Versus Security Assessment Tool[75].”

[GSCTool 2002] O’Neill, Don, “Global Software Competitiveness Assessment Tool[76].”

[NSQE Assess] “Software Inspection Measurements and Derived Metrics[77].”

[SecROI Tool 2006] O’Neill, Don, “Security Return on Investment Interactive Worksheet[78].”

Bibliography

[Baker 2008] “Homeland Security Enforcement Priorities and Policies.” Presentation at Corporate Compliance in the Global Environment, a Baker & McKenzie conference, Washington, D.C., February 7, 2008.

[Caralli 2006] Caralli, Richard A., Stevens, James. F., Wallen, Charles M., & Wilson, William R. *Sustaining Operational Resiliency: A Process Improvement Approach to Security Management* (CMU/SEI-2006-TN-009[79]). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, April 2006.

[Caralli 2007] Caralli, Richard A., Stevens, James. F., Wallen, Charles M., White, David W., Wilson, William R., & Young, Lisa R. *Introducing the CERT Resiliency Engineering Framework: Improving the Security and Sustainability Processes* (CMU/SEI-2007-TR-009[80]). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, May 2007.

[CMMI 2006] CMMI Product Team. *CMMI for Development, Version 1.2* (CMU/SEI-2006-TR-008[81]). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, August 2006.

[CNSS 2005] Center for National Software Studies. “Software 2015[82]: A National Software Strategy to Ensure U.S. Security and Competitiveness,” May 2005.

[COC 2002] “Creating Opportunity Out of Adversity: Proceedings of the National Symposium on Competitiveness and Security.” Council on Competitiveness, Pittsburgh, Pennsylvania, October 8-9, 2002.

[COC 2007] Council on Competitiveness. “Competitiveness Index: Where America Stands.” Washington, D.C., 2007 (ISBN 1-889866-31-8).

[Collins 2005] Collins, Rosann W., Walton, Gwendolyn H., Hevner, Alan R., & Linger, Richard C. *The CERT Function Extraction Experiment: Quantifying FX Impact on Software Comprehension and Verification* (CMU/SEI-2005-TN-047[83]). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, December 2005.

[CSTB 2007] Computer Science and Telecommunications Board. “Toward a Safer and More Secure CyberSpace.” CTSB, The National Academies Press, 2007.

[DACS 2006] “Future Directions in Software Engineering[84].” *Software Tech* 10, 3 (October 2007).

[DHS 2003] Department of Homeland Security. “National Strategy to Secure Cyberspace[85], Action-Recommendation 2-14,” February 2003.

[DHS 2006] “Security in the Software Life Cycle”, Draft Version 1.2, Department of Homeland Security, August 2006.

[Ellison 1997] Ellison, R. J., Fisher, D. A., Linger, R. C., Lipson, H. F., Longstaff, T., & Mead, N. R. *Survivable Network Systems: An Emerging Discipline* (CMU/SEI-97-TR-013[87]). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, November 1997 (revised May 1999).

[EMP 2004] Report of the Commission[88] to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, 2004.

[Gansler 2004] Gansler, Jacques S. & Binnendijk, Hans. “Information Assurance: Trends in Vulnerabilities, Threats, and Technologies.” National Defense University, Center for Technology and National Security Policy, Washington, D.C., 2004.

[Goodenough 2007] Goodenough, John, Lipson, Howard, & Weinstock, Chuck. “Arguing Security - Creating Security Assurance Cases[89].” Build Security In, January 2007.

[Hoglund 2004] Hoglund, Greg & McGraw, Gary. *Exploiting Software: How to Break Code*. Pearson Education, Inc., 2004 (ISBN: 0-201-78695-8).

[Humphrey 2006] Humphrey, Watts. *Systems of Systems: Scaling Up the Development Process* (CMU/SEI-2006-TR-017[90]). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, August 2006.

[Jackson 2007] Jackson, Daniel, Thomas, Martyn, & Millett, Lynette I. “Software for Dependable Systems: Sufficient Evidence?” National Research Council of the National Academies (ISBN: 0-309-10857-8).

[Larstan 2005] Larstan. *The Black Book on Corporate Security*. Potomac, MD: Larstan Publishing Inc., 2005 (ISBN: 0-9764266-1-7).

[Linger 2001] Linger, Richard C. & Moore, Andrew P. *Foundations for Survivable System Development: Service Traces, Intrusion Traces, and Evaluation Models* (CMU/SEI-2001-TR-029[91]). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, October 2001.

[Miller 2008] Miller, Robert A. & Lachow, Irving. “Strategic Fragility[92]: Infrastructure Protection and National Security in the Information Age.” *Defense Horizons*, Number 59 (January 2008). Center for Technology and National Security Policy, National Defense University.

[O’Neill 1998] O’Neill, Don. “Global Software Competitiveness Maturity Model[93].” *The Competitor 1*, 4 (March 1998).

[O’Neill 2003] O’Neill, Don. “CSO Leadership Program[94].” *The Competitor 6*, 3 (January 2003).

[O’Neill 2004a] O’Neill, Don. “Competition Versus Security[95].” *CrossTalk*, June 2004.

[O’Neill 2004b] Don O’Neill. “Inside Track to Offshore Outsourcing[97].” *The Competitor 7*, 4 (March 2004).

[O’Neill 2006a] O’Neill, Don. “Criteria and Guidance for Peer Review of Open Source Artifacts[98].” *The Competitor 10*, 1 (September 2006).

[O’Neill 2006b] O’Neill, Don. “Canonical Model for Expressing a Statement of Electronic-based Critical Infrastructure Sector Dependency[99].” *The Competitor 10*, 2 (November 2006).

[O’Neill 2007a] O’Neill, Don. “Business Considerations and Foundations for Transforming and Assuring Software Security[100]: Business Case Models for Rational Action.” Build Security In, February 2007.

[O’Neill 2007b] O’Neill, Don. “Calculating Security Return on Investment[101].” Build Security In, February 2007.

[Perelman 2006] Perelman, Lewis J. “Shifting Security Paradigms Toward Resilience.” George Mason University School of Law, October 2006.

[Phoha 2006] Phoha, Shashi, La Porta, Thomas, & Griffin, Christopher (Eds.). *Sensor Network Operations*. Wiley-IEEE Press, 2006 (ISBN-13 978-0-471-71976-2).

[SEI 2006] *Ultra-Large-Scale Systems: The Software Challenge of the Future*[102]. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, July 2006 (ISBN 0-9786956-0-7).

[USPTO 2004] Title of invention “Business management and procedures involving intelligent middleman”, Inventor Donald O’Neill, Publication Number US20060015384 A1, Submission Date July 14, 2004.

[Van Opstel 2007] Van Opstel, Debra. “The Resilient Economy: Integrating Competitiveness and Security.” Council on Competitiveness, Washington, D.C., 2007, (ISBN 1-889866-33-4).

Carnegie Mellon Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[1] mailto:permission@sei.cmu.edu